

IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the present application:

1-14. (Canceled)

15. (Previously presented) A method comprising:

operating a primary trusted provisioning domain (TPD); and

using the primary TPD to provision a mobile device on a wireless network by sending a provisioning message to the mobile device, the provisioning message specifying a secondary TPD authorized to provision the mobile device via a network and an identifier of one or more parameters which the secondary TPD is authorized to provision, the secondary TPD comprising a provisioning server.

16. (Original) A method as recited in claim 15, wherein the primary TPD is within a trusted environment, and wherein the secondary TPD is outside the trusted environment.

17. (Original) A method as recited in claim 16, wherein the secondary TPD communicates with the mobile device via a second network that is outside the trusted environment.

18. (Original) A method as recited in claim 16, further comprising using the primary TPD system to provision the mobile device with a digital certificate identifying the secondary TPD to enable the secondary TPD to provision the mobile device using a digital signature.

19. (Original) A method as recited in claim 15, wherein the provisioning message specifies a plurality of secondary TPDs authorized to provision the mobile device and one or more parameters which each of the secondary TPDs is authorized to provision.

20. (Original) A method comprising:

operating a primary provisioning server within a predefined trusted environment, the primary provisioning server having authorization to provision a plurality of mobile devices on a wireless network;

using the primary provisioning server to provision a digital certificate of the primary provisioning server in each of the mobile devices;

using the primary provisioning server to provision a digital certificate of a secondary provisioning server in the mobile devices, wherein the secondary provisioning server is on a second network outside the trusted environment; and

using the primary provisioning server to provision the mobile devices with information indicating to the mobile devices authorization of the secondary provisioning server to provision the mobile devices.

21. (Original) A method as recited in claim 20, wherein the primary and secondary provisioning servers each use their respective digital certificates when provisioning the mobile devices, to enable the mobile devices to authenticate provisioning messages from the primary and secondary provisioning servers.

22. (Original) A method as recited in claim 20, further comprising using the primary provisioning server to specify one or more parameters which the secondary provisioning server is authorized to provision in the mobile devices.

23. (Original) A method as recited in claim 20, further comprising using the primary provisioning server to provision the mobile devices with information indicating authorization of a plurality of secondary provisioning servers to provision the mobile devices.

24. (Original) A method as recited in claim 23, further comprising using the primary provisioning server to specify one or more parameters which each of the secondary provisioning servers is authorized to provision in the mobile devices.

25. (Original) A method as recited in claim 24, wherein said using the primary provisioning server to specify one or more parameters comprises assigning each of the secondary provisioning servers provisioning authorization of a different scope.

26. (Original) A method as recited in claim 20, wherein the primary provisioning server has unrestricted authorization to provision the mobile devices, and authorization of the secondary provisioning server to provision the mobile devices is regulated by the primary provisioning server.

27-31. (Canceled)

32. (Original) A machine-readable program storage medium storing instructions which, when executed in a processing system, configure the processing system to operate as a primary provisioning server within a predefined trusted environment, the primary provisioning server having authorization to provision a plurality of mobile devices on a wireless network, such that the instructions configure the processing system to execute a process comprising:

provisioning a digital certificate of the primary provisioning server in each of the mobile devices;

provisioning a digital certificate of a secondary provisioning server in the mobile devices, wherein the secondary provisioning server operates outside the trusted environment; and

provisioning the mobile devices with information indicating to the mobile devices authorization of the secondary provisioning server to provision the mobile devices.

33. (Original) A machine-readable program storage medium as recited in claim 32, wherein the primary and secondary provisioning servers each use their respective digital certificates when provisioning the mobile devices, to enable the mobile devices to authenticate provisioning messages from the primary and secondary provisioning servers.

34. (Original) A machine-readable program storage medium as recited in claim 32, wherein the process further comprises specifying one or more parameters which the secondary provisioning server is authorized to provision in the mobile devices.

35. (Original) A machine-readable program storage medium as recited in claim 32, wherein the process further comprises provisioning the mobile devices with information indicating authorization of a plurality of secondary provisioning servers to provision the mobile devices.

36. (Original) A machine-readable program storage medium as recited in claim 35, wherein the process further comprises specifying one or more parameters which each of the secondary provisioning servers is authorized to provision in the mobile devices.

37. (Original) A machine-readable program storage medium as recited in claim 36, wherein said specifying one or more parameters comprises assigning each of the secondary provisioning servers provisioning authorization of a different scope.

38. (Original) A machine-readable program storage medium as recited in claim 32, wherein the primary provisioning server has unrestricted authorization to provision the mobile devices, and authorization of the secondary provisioning server to provision the mobile devices is regulated by the primary provisioning server.

39. (Canceled)

40. (Previously presented) A method of operating a mobile device on a wireless network, the method comprising:

receiving a provisioning message from a first trusted provisioning domain (TPD), the provisioning message specifying a second TPD and indicating a parameter which the second TPD is authorized to provision in the mobile device, the secondary TPD comprising a provisioning server;

storing information identifying the second TPD and the parameter in response to the provisioning message; and

provisioning the parameter in the mobile device in response to a provisioning message received over a network from the second TPD.

41. (Original) A method as recited in claim 40, wherein the first TPD is within a trusted environment, and the second TPD is outside the trusted environment.

42. (Original) A method as recited in claim 41, further comprising:

receiving a digital certificate of the second TPD from the first TPD; and

using the digital certificate in the mobile device to authenticate the provisioning message from the second TPD.

43. (Original) A method as recited in claim 40, wherein the provisioning message specifies a plurality of secondary TPDs and a parameter which each of the secondary TPDs is authorized to provision in the mobile device, the method further comprising storing information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message.

44. (Original) A method of operating a mobile device on a wireless network, the method comprising:

receiving a provisioning message from a remote source, the provisioning message specifying a parameter;

determining whether the remote source is a primary trusted provisioning domain (TPD);

if the remote source is the primary TPD, provisioning the parameter in the mobile device in response to the provisioning message;

if the remote source is not the primary TPD, determining whether the remote source is a secondary TPD authorized to provision the parameter, based on a provisioning authorization previously received by the mobile device from the primary TPD; and

if the remote source is a secondary TPD authorized to provision the parameter, provisioning the parameter in the mobile device in response to the provisioning message.

45. (Original) A method as recited in claim 44, wherein the primary TPD operates within a trusted environment, and the secondary TPD operates outside the trusted environment.

46. (Original) A method as recited in claim 44, further comprising:

receiving a digital certificate of the secondary TPD from the primary TPD; and

using the digital certificate in the mobile device to authenticate the provisioning message.

47. (Original) A method as recited in claim 44, wherein the provisioning message specifies a plurality of secondary TPDs and a parameter which each of the secondary TPDs is authorized to provision in the mobile device, the method further comprising storing information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message.

48. (Original) A mobile device configured to operate on a wireless network, the mobile device comprising:

a processor;

a data communication device coupled to the processor to communicate data with one or more remote systems via the wireless network; and

a memory coupled to the processor and storing instructions for execution by the processor to configure the mobile device to execute a process comprising

receiving a provisioning message from a first trusted provisioning domain (TPD) via the wireless network, the provisioning message specifying a second TPD and indicating a parameter which the second TPD is authorized to provision in the mobile device;

storing information identifying the second TPD and the parameter in response to the provisioning message; and

provisioning the parameter in the mobile device in response to a provisioning message from the second TPD.

49. (Original) A mobile device as recited in claim 48, wherein the first TPD is within a trusted environment, and the second TPD is outside the trusted environment.

50. (Original) A mobile device as recited in claim 49, wherein the process further comprises:

receiving a digital certificate of the second TPD from the first TPD; and

using the digital certificate in the mobile device to authenticate the provisioning message from the second TPD.

51. (Original) A mobile device as recited in claim 48, wherein the provisioning message specifies a plurality of secondary TPDs and a parameter which each of the secondary TPDs is authorized to provision in the mobile device, and wherein the process further comprises storing information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message.

52. (Original) A mobile device configured to operate on a wireless network, the mobile device comprising:

- a processor;

- a data communication device coupled to the processor to communicate data with one or more remote systems via the wireless network; and

- a memory coupled to the processor and storing instructions for execution by the processor to configure the mobile device to execute a process comprising

- receiving a provisioning message from a remote source, the provisioning message specifying a parameter;

- determining whether the remote source is a primary trusted provisioning domain (TPD);

- if the remote source is the primary TPD, provisioning the parameter in the mobile device in response to the provisioning message;

- if the remote source is not the primary TPD, determining whether the remote source is a secondary TPD authorized to provision the parameter, based on a provisioning authorization previously received by the mobile device from the primary TPD; and

- if the remote source is a secondary TPD authorized to provision the parameter, provisioning the parameter in the mobile device in response to the provisioning message.

53. (Original) A mobile device as recited in claim 52, wherein the primary TPD operates within a trusted environment, and the secondary TPD operates outside the trusted environment.

54. (Original) A mobile device as recited in claim 52, wherein the process further comprises:

- receiving a digital certificate of the secondary TPD from the primary TPD; and

- using the digital certificate in the mobile device to authenticate the provisioning message.



55. (Original) A mobile device as recited in claim 52, wherein the provisioning message specifies a plurality of secondary TPDs and a parameter which each of the secondary TPDs is authorized to provision in the mobile device, and wherein the process further comprises storing information identifying each of the secondary TPDs and the corresponding parameters in response to the provisioning message.